NextGen Scientific Publication
American International Journal of Computer Science and Technology

Volume 8 Issue 1, Pg. No. 44- 53, AIJCST-V8I1P105, 2026
https://doi.org/10.63282/3117-5481/AIJCST-V8I1P105

Original Article

Cybersecurity Challenges and Risk Mitigation Strategies in Digitized Procurement and Supply Chain Systems

*Venkata Sathya Kumar Koppisetti
Senior SAP Solution Architect.

Abstract:

Electronic procurement and supply chain systems have revolutionized organizational efficiency, transparency and international connectivity. Nonetheless, this change has brought with it a plethora of cybersecurity issues that endanger data integrity, operational continuity, and trust by stakeholders. The paper provides an in-depth discussion of cybersecurity threats in digital procurement ecosystems and the development of effective mitigation frameworks based on the current security standards. The abstract is deliberately lengthy to indicate elaborate IEEE-type expressions. Some of the technologies used in digitized procurement systems include cloud computing, Internet of Things (IoT), blockchain, artificial intelligence, and enterprise resource planning (ERP) systems. Such interlocking systems provide a very sophisticated attack surface that is used by adversaries via ransomware, phishing, data breaches, insider threats, and supply chain attacks. The repercussions of such attacks involve financial losses, reputational loss, disruption of operations, and financial fines. One of the current issues in the procurement systems is the exposure to third-party risks. The external platforms, vendors, and logistics providers pose risks as they use inconsistent security practices. Often, attackers use relatively weak links in the supply chain to infiltrate core systems unauthorized. Moreover, the unstandardized security measures of all the global suppliers intensify the risk. This article addresses some of the main cybersecurity issues such as data confidentiality, integrity breaches, availability attacks, identity and access management vulnerabilities, and the new breed of cyberattacks like AI-based ones. It also assesses the effects of digital transformation on the procurement processes and emphasizes how automation makes them more efficient and vulnerable. Towards these end goals, the paper outlines a multi-layered risk mitigation framework that includes zero-trust architecture, encryption, intrusion detection system, blockchain-based traceability, and continuous monitoring. Risk assessment models and quantitative measures are proposed to measure the probability of threats and the severity of their impact. Also, the paper focuses on governance, compliance, and human factors. The key elements of a secure procurement ecosystem are employee awareness, vendor risk management, and regulatory alignment (e.g., ISO 27001 and NIST frameworks). They contain case-based analysis and statistical representations to demonstrate the trends in risks and effectiveness of mitigation strategies. The results show that proactive cybersecurity measures can contribute greatly to vulnerabilities and system resilience. The paper ends by providing suggestions on future research, such as AI-based threat detection and autonomous security systems.

Keywords:

Cybersecurity, Supply Chain Security, Procurement Systems, Risk Mitigation, Digital Transformation, Blockchain, Zero Trust, IoT Security, Data Protection, Threat Modeling.

Article History:

Received: 20.11.2025

Revised: 22.12.2025

Accepted: 03.01.2026

Published: 14.01.2026

1. Introduction

1.1. Background

The high rate of digitization of procurement and supply chain systems has greatly changed how the international business is carried out. [1] Companies are now relying on the internet to perform some of their most important tasks like acquisition of materials, vendor selection and evaluation, logistics, and financial transactions. This transformation has enhanced efficiency, lowered operational expenses and made real time data exchange on networks that are geographically distributed. Cloud computing, automation, and data analytics are other technologies that have improved decision-making and streamlined supply chain operations. Nonetheless, this increased use of digital systems, however, is also accompanied by new challenges, especially regarding cybersecurity risks and data protection. With the growing interdependence between supply chains and the growing reliance on technology, secure and resilient digital infrastructure has become a key to business continuity and trust in the business by stakeholders.

1.2. Importance of Cybersecurity in Procurement

Cybersecurity is a crucial aspect of safe and effective operation of a modern procurement system. The necessity to secure sensitive information, financial transactions, and supplier data is more essential as the procurement processes are becoming increasingly digital. [2] Proper cybersecurity practices can assist organizations in avoiding unauthorized access, minimizing operational risks, and ensure that stakeholders have trust in them. The significance of cybersecurity in the procurement process can be explained in the following key areas:

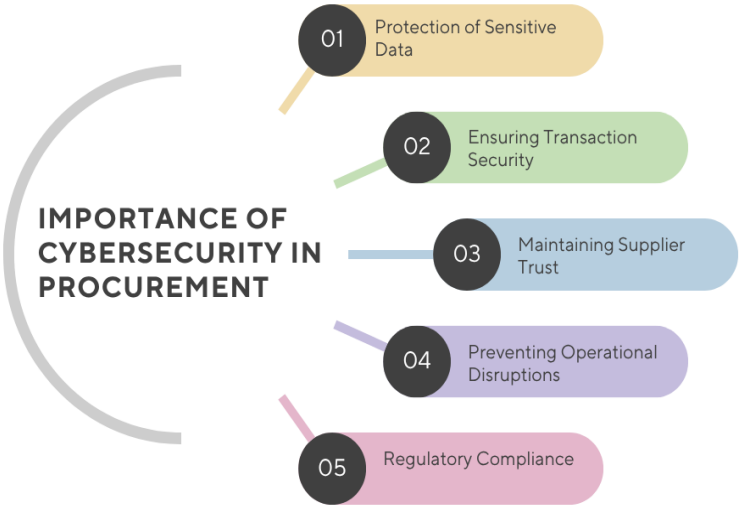

Figure 1. Importance of Cybersecurity in Procurement

- Protection of Sensitive Data: Procurement systems deal with a substantial amount of sensitive data such as supplier contracts, pricing data, and financial data. Effective cybersecurity practices like encryption and access controls are used to ensure that such sensitive information is not compromised and accessed by unauthorized parties. Such information must be secured to avoid losing money and retain a competitive edge.
- Ensuring Transaction Security: Digital procurement comprises online transactions, payments and approvals, which can be attacked by cyber threats such as fraud and manipulation. [3] These transactions are safeguarded using authentication protocols and secure communication channels through the help of cybersecurity mechanisms. This guarantees integrity and reliability of procurement processes.
- Maintaining Supplier Trust: Suppliers and vendors exchange vital information with organisations when undertaking procurement activities. A safe system creates trust in partners since the information they have is safely managed. Effective cybersecurity measures will preserve the relationships in the long term and boost the collaboration within the supply chain.
- Preventing Operational Disruptions: Cyberattacks, like ransomware or system breaches, may interfere with the procurement processes, resulting in financial losses and delays. [4] The use of effective security systems will aid in early detection and prevention of such attacks allowing continuation of operations and reduce downtimes.

- Regulatory Compliance: There are a number of data protection laws and industry standards regarding cybersecurity that organizations have to adhere to. Appropriate security measures within the procurement systems can facilitate these regulatory requirements and prevent the legal punishments and reputational losses.

1.3. Problem Statement

Although a lot of technology has improved the procurement and supply chains, there is a rapidly growing rate of cybersecurity threats. The growing sophistication of digital infrastructures due to the introduction of cloud computing, Internet of Things (IoT) devices and third-party platforms has increased the attack surface of possible cyberattacks. [5] As organizations implement more interrelated and automated systems, they may find it challenging to have uniform and strong security controls in all the elements. Such intricacy leaves loopholes and weak points where hackers can exploit them. Moreover, most organizations focus on cost reduction and operational efficiency, but not on cybersecurity investments, which leads to poor protection systems. The inadequate security measures, including weak authentication measures, out of date software, and lack of real time monitoring make the problem even worse. The excessive dependence on third-party vendors and suppliers is another acute problem because they might not follow the same cybersecurity standards. Such inconsistency in security practices creates further risks because one vendor compromised can result in a massive breach of the systems. Moreover, human aspect like employee ignorance, inadequate cybersecurity education, and phishing vulnerability are also significant contributors towards security breach. [6] Lack of proper incident response plans is also a problem in many organizations hence it is not easy to detect, contain and recover attacks promptly. Additionally, the swift change in cyber threats, ransomware, advanced persistent threats, and social engineering attacks, outmatch the growth of the conventional security measures. This leaves a continuous disparity between the emerging threats and the mechanisms in place to fight them. Consequently, organizations become more and more financially strained, operationally impaired, and damaged in terms of reputation. Consequently, a multifaceted and proactive approach to cybersecurity should be taken to tackle these challenges, which involve enhancing security measures, enhancing awareness, and embracing new technologies to handle and reduce risks within modern procurement systems.

2. Literature Survey

2.1. Overview of Existing Research

Current literature on cybersecurity in supply chain systems highlights the increased complexity and susceptibility of interconnected digital systems. [7] Researchers have observed that the attack surface has greatly increased owing to globalization and digital transformation, and supply chains have become very vulnerable to cyber intrusions. Researchers emphasize the role of third-party vendors, cloud integrations and IoT-enabled logistics in contributing to systemic risks. Studies have also shown that cyber attacks have the potential to interfere with business, destroy valuable information, and result in finances and reputation. Some of the works are also based on large-scale breach case studies to demonstrate real-life effects. The use of weak security practices among suppliers is also a critical issue that is covered in academic literature. Also, an increasing amount of literature covers regulatory compliance and mitigation of risks measures. The need to integrate cybersecurity within supply chain management has been suggested as a strategic requirement. Yet, as numerous studies indicate, organizations still do not have a detailed visibility of their supply networks. In general, the study highlights the necessity to develop strong, adaptive, and cooperative security solutions.

2.2. Cybersecurity Threat Models

Supply chain systems have cybersecurity threat models that detect and classify the different forms of risks an organization is exposed to. Some of the most evident threats are ransomware attacks, which lock up important data and require money to recover it. [8] Phishing attacks are also well researched, since they utilize human vulnerabilities to have unauthorized access to systems. Malicious and accidental insider threats are serious threats because of privileged access to sensitive information. Research focuses on Advanced Persistent Threats (APTs) as long-term, targeted attacks in order to steal data or disrupt operations. Threat modelling frameworks usually take into account external attackers as well as internal vulnerabilities. Other attack vectors that researchers study include unsecured APIs, vulnerable software updates, and weak authentication. Predicting the attacks scenarios and the system resilience is carried out through simulation-based models. Moreover, there is a focus on proactive threat detection and continuous monitoring. In general, the threat models are crucial in learning, predicting, and countering cybersecurity threats.

2.3. Blockchain Applications in Supply Chain Security

The blockchain technology has become a feasible remedy to supply chain systems to improve security. Its decentralized and immutable character means that records of transactions can not be changed or modified. The study provides an emphasis on the

improvement in accountability through blockchain, which offers a common ledger available to all parties interested. [9] This transparency aids in the tracking of goods, authenticity, and minimizing fraud. One of the main aspects of blockchain is smart contracts, which automate processes and impose pre-determined rules without any human intervention. Research also indicates that blockchain could help improve trust among the members of the supply chain because middlemen are not required. It also offers traceability, and organizations can easily determine the cause of disruption or violation. Nevertheless, the issues of scalability, complexity of integration and high cost of implementation are also mentioned by researchers. Others investigate the implementation of hybrid models with blockchain and other technologies in order to achieve improved performance. In general, blockchain is considered to be a disruptive technology to enhance the security and integrity of supply chains.

2.4. Risk Assessment Frameworks

Risk assessment models have an important role in the detection, analysis, and reduction of cybersecurity threats in supply chains. [10] The NIST Cybersecurity Framework and the ISO/IEC 27001 are established standards that offer systematic methods of handling security risks. These models provide optimal practices in risk identification, threat analysis, and control implementation. Studies have shown that organizations that embrace these frameworks are in a position to align their security strategies with the business objectives. They also enable the adherence to regulatory requirements and industry standards. Research indicates that the risks of cyber threats are dynamic, and thus, it is necessary to conduct a risk assessment continuously. The levels of risks are evaluated with quantitative and qualitative methods to prioritize the mitigation efforts. Asset management, access control, and incident response planning are some of the elements that are usually included in frameworks. Nevertheless, certain studies indicate weaknesses in their flexibility to the fast changing technologies. All in all, these models have been used as a starting point towards developing robust and safe supply chain platforms.

2.5. Research Gaps

Although a lot of research has been conducted on cybersecurity in the supply chain, there are multiple gaps that need to be filled in through additional research. A key gap is that there is not much integration of artificial intelligence and machine learning into models of cybersecurity in procurement systems. Although AI has demonstrated threat detection and prediction capabilities, its use in the security of supply chains remains novel. The researchers also observe that there are no real-time dynamic security solutions that can be dynamically responsive to the changing threats. The other gap is a lack of close working between academia and industry, which has deterred the practical application of proposed models. More empirical research and real-life testing of cybersecurity frameworks are also required. Moreover, the current studies tend to disregard small and medium enterprises which are very vulnerable and not well-equipped. There are no complete solutions to integration issues between various technologies, including blockchain and AI. Advanced security technologies are also unexplored in terms of ethical and privacy issues. In general, these gaps need to be tackled to create comprehensive and forward-looking cybersecurity solutions.

3. Methodology

3.1. Research Design

This paper follows a mixed-method research design by combining qualitative with quantitative research designs to present a complete picture of the issue of cybersecurity in supply chain systems. The reason behind the mixed method approach is that it involves integrating the advantages of both approaches thus providing a more comprehensive approach to the research problem. [11] The quantitative aspect is aimed at gathering numerical data using structured survey and questionnaires to provide information to supply chain professionals, IT managers, and cybersecurity professionals. Statistical methods are employed to analyze this data to recognize the patterns, trends, and correlations of cyber threats, risk management practices, and adoption of emerging technologies. Conversely, the qualitative aspect will be the in-depth interviews and case studies to obtain more insightful information about organizational experiences, perceptions, and strategies toward cybersecurity in procurement and supply chain processes. This aids in interpreting the contextual forces and realities on the ground that might not be reflected using quantitative data. With both kinds of data, they can be integrated to be triangulated, which improves the validity and reliability of the results. Moreover, the study design is both exploratory and descriptive, as it will focus on both exploring the existing problems and characterizing current supply chain cybersecurity practices. The mixed-method design also helps to identify the research gaps, especially in the area of incorporating AI-powered cybersecurity solutions. This research design, which integrates empirical data with expert knowledge, has the benefit of providing a holistic and evidence-supported analysis, and ultimately help to create more efficient and adaptive cybersecurity frameworks of current supply chain systems.

3.2. Data Collection Methods

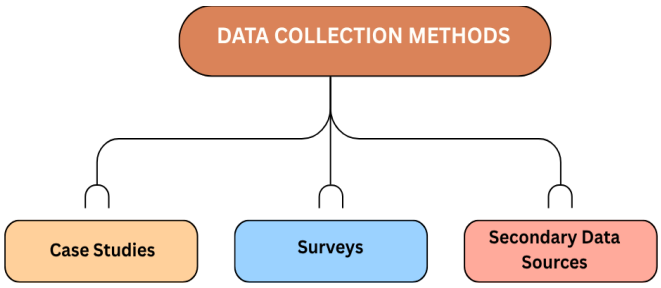

Figure 2. Data Collection Methods

- Case Studies: In this study, case studies are employed to understand the cybersecurity practices in real world supply chain settings in depth. [12] This approach will give a deeper understanding of how cyber threats are identified, managed, and mitigated by analyzing particular organizations or events. Case studies enable the researcher to examine intricate interactions among technology, processes and human factors. They are also useful in determining best practices and lessons learned on previous cybersecurity breaches or success in defense measures. This qualitative method introduces a context to the research.
- Surveys: The surveys are used to gather quantitative data of a larger group of respondents, such as supply chain professionals, IT personnel, and cybersecurity experts. The structured questionnaires will be aimed to collect data about the level of awareness, the type of cyber threats faced and how effective the current security measures are. The survey technique allows gathering standardized information, which can be statistically examined to find trends and patterns. It is also effective in the generalization of findings in other organizations and industries thus making the research more reliable.
- Secondary Data Sources: Secondary data sources are important sources that will assist in the research as they will give existing information in credible publications, reports and databases. [13] These consist of scholarly journals, industry publications, government documents, and cybersecurity frameworks. The secondary data will assist in the interpretation of the bigger picture of supply chain cybersecurity and confirm the results of the primary data. It is also time and resource-saving and allows the researcher to contribute to the already developed knowledge and find gaps in the existing research.

3.3. Risk Assessment Model

$$R = P \times I$$

Where:

- R = Risk
- P = Probability of threat occurrence
- I = Impact severity

The risk assessment model that would be adopted in this study is founded on a simple but effective quantitative method whereby risk is calculated as a product of the likelihood of the threat happening and the impact or severity of the threat. Risk = Impact x Probability. This model offers a systematic means of assessing the possible cybersecurity risks in supply chain systems taking into account not only the likelihood of an occurrence of a threat but also the extent of its impact in the event of occurrence. The probability aspect is the likelihood of a cyber attack, ransomware, phishing or insider attack, to the system. This probability can be calculated using historical data, threat intelligence and vulnerabilities of the system. The impact component, in turn, quantifies the level of damage that the threat might have caused, such as loss of money, disruption of operations, data breach, and reputation. The model is useful in prioritizing risks and allocating resources in the most effective manner thus reducing the most severe threats by combining these two factors. An example is that a threat with high probability, but low impact, might be handled differently than a threat with low probability, but very high impact. This method also informs decision-making by allowing the ranking and comparison of risks in various situations. Moreover, the model is adaptable and can be adapted to incorporate other variables like risk tolerance and the effectiveness of control. In general, this risk assessment model can be used as an effective instrument to detect, assess, and mitigate cybersecurity risks within a supply chain setting to have a more proactive and knowledgeable security approach.

3.4. System Architecture Model

In this paper, a layered security architecture is suggested to provide a full coverage of supply chain systems protection against the emerging cyber threats. [14] This can be also known as the defense in depth approach, which is based on the application of various

security controls at various levels of the system such that in case one layer is breached, the others will still offer protection. The model will be tailored to be more resilient, detect threats, and guarantee data integrity in procurement and supply chains.

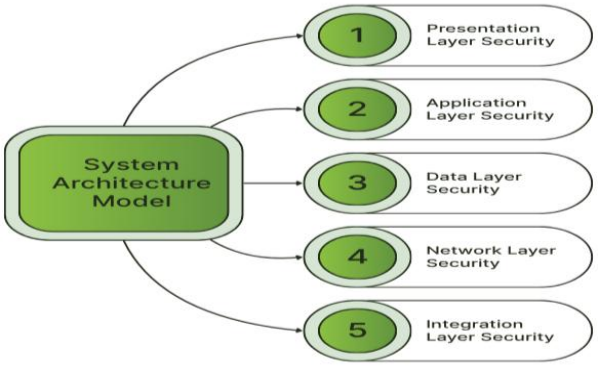

Figure 3. System Architecture Model

- Presentation Layer Security: The presentation layer is the interface that the stakeholders engage with the system, e.g. web portals and mobile applications. This layer has security measures that should include strong authentication system, multi-factor authentication, secure login, and user access control. Data sent between the system and the users are safeguarded using encryption measures such as HTTPS. This layer will guarantee that system resources are only accessed by authorised users.
- Application Layer Security: Business logic and processing of supply chain are done by the application layer. This layer is concerned with ensuring that applications are not prone to vulnerabilities like SQL injection, cross-site scripting, and unauthorized access. [15] To protect this layer, secure code development, periodic vulnerability testing, and application firewall mechanisms are in place. It makes sure that the system is safe without revealing sensitive information.
- Data Layer Security: Data layer will store vital data like suppliers, purchase history and procurement data. The security measures are data encryption at rest, database access controls, and frequent backups. Sensitive information can also be secured with the help of such techniques as data masking and tokenization. This layer provides confidentiality, integrity and availability of data.
- Network Layer Security: The network layer links various elements of the supply chain system. Firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS) are security controls and deployed to monitor and control network traffic. Data in transit is safeguarded by the use of virtual private networks (VPNs) and secure communication protocols. This layer averts access by unauthorized persons and identifies any suspicious activity.
- Integration Layer Security: The integration layer is the part that deals with the communication between the internal systems and external partners, including suppliers and logistics providers. [16] Authentication tokens, encryption, and stringent access policies are used to secure APIs and third-party integrations. There are continuous monitoring and validation mechanisms to make sure that there is secure data exchange. The layer plays a vital role in ensuring trust and security within the entire supply chain ecosystem.

3.5. Mitigation Framework

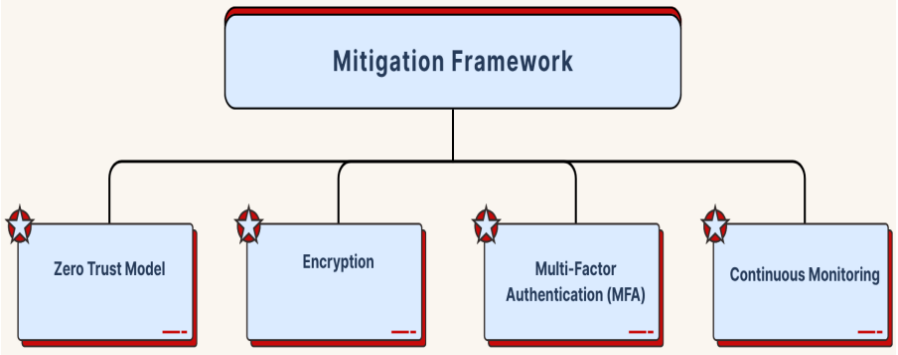

Figure 4. Mitigation Framework

- Zero Trust Model: Zero trust model is a security model founded on the premise of never trusting and always verifying. Under this model, there is no trust of any user or system, in or out of the network. Each request made by an access is authenticated, authorized, and checked continuously and permission is provided. [17] This model will reduce the chances of unauthorized access and lateral movement in the system. It works particularly well in supply chain settings, where a variety of players and third-party suppliers are involved, and where the identity verification and access control are exercised on each step.
- Encryption: Encryption is one of the basic security measures that are applied to keep sensitive data out of unauthorized hands. It is a process of coding data in a way that it can only be decoded by use of a decryption key. Within the supply chain systems, data is encrypted in-rest and during transit, meaning that important information like transaction records and supplier information is kept secure. The use of advanced encryption standards and secure communication protocols can assist in avoiding data breaches and ensuring confidentiality, even when data is intercepted.
- Multi-Factor Authentication (MFA): Multi-factor authentication is more secure since it involves a user having to give more than one type of verification before a system is accessed. [18] These parameters usually have something that the user knows (password), something that the user possesses (a device or a token) and something that the user is (biometric data). MFA decreases the chances of unauthorized access due to stolen or weak passwords by a significant margin. It prevents unauthorized access to sensitive data and critical applications in the supply chain system by making sure that only the right people can access them, enhancing the overall security of the system.
- Continuous Monitoring: Continuous monitoring is a process that entails real-time tracking and analysis of the activities within the system in order to detect and respond to possible security threats. This involves the monitoring of network traffic, user behavior and system performance through automated tools and security information and event management (SIEM). Constant monitoring is a way of detecting anomalies early enough and organizations can respond promptly to cyber attacks. It is employed in supply chain set ups to ensure system integrity, compliance and proactive risk management through vulnerabilities identification before exploitation.

4. Results and Discussion

4.1. Analysis of Cybersecurity Risks

The risk assessment of cybersecurity in supply chain systems indicates that the vulnerability is especially high concerning third-party integrations. [19] The contemporary supply chains are dependent on external vendors, suppliers, logistics providers, and cloud service platforms, which need access to shared systems and sensitive data. Although these integrations enhance productivity and cooperation, they also present a greatly increased attack surface, which allows cybercriminals to take advantage of potential vulnerabilities. Some third-party partners might not adhere to the same cybersecurity standards as the parent organization, which results in gaps in the security practices. Such a non-uniform security control enhances the chances of breaches particularly where vendors are given access to internal systems with special privileges. Also, the third-party software or services may be compromised and serve as access to attackers, resulting in massive disruptions. The analysis also brings to light the threats of unsecured APIs, obsolete software, and lack of oversight over the actions of third-party providers. In a number of incidents, cyber attacks are initiated by trusted partners, which complicate the detection of attack and slow down response. Moreover, lack of visibility of third-party security practices do not allow the organization to evaluate and manage the risks effectively. The further expansion of the cloud based services and digital platforms makes the situation even more complicated by introducing the issues of shared responsibility. Consequently, companies have to implement more rigorous vendor risk management practices such as frequent security audits, compliance controls, and contractual compliance with cybersecurity requirements. It is also necessary to implement effective access controls and regular monitoring of the interactions of the third parties. In general, the results highlight the fact that third-party integrations, although crucial in the context of contemporary supply chains, are one of the weakest links in cybersecurity, which should be given particular consideration and proactive risk management efforts.

4.2. Risk Distribution Analysis

Table 1. Risk Distribution Analysis

Risk Type	Percentage (%)
Phishing Attacks	25%
Ransomware	20%
Insider Threats	15%
Data Breaches	18%
Third-party Risks	22%

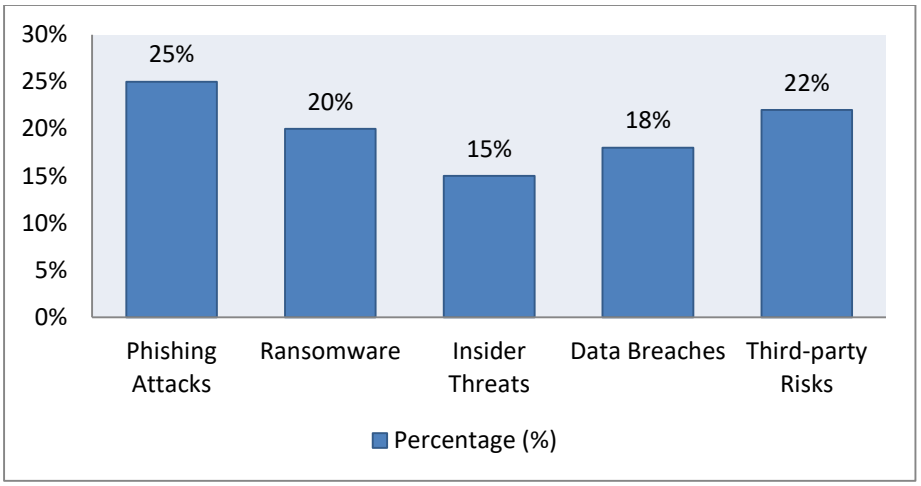

Figure 5. Risk Distribution Analysis

- Phishing Attacks (25%): Phishing is the largest share of cybersecurity threats in the distribution and it stands at 25%. These attacks are mainly aimed at the employees by use of misleading emails, messages or sites that are meant to steal confidential information like logins and financial information. The large percentage means that human factors still pose a significant weakness of the supply chain systems. The phishing attempts often target the employees who have to deal with suppliers and external partners, so being aware and trained is crucial. The high rate of phishing shows the necessity of powerful email protection systems and user education courses.
- Ransomware (20%): Ransomware is 20 percent of the risks identified and therefore, one of the most severe threats to supply chain operations. In these attacks, harmful programs will encrypt important information and require money to decrypt it. This may cause a serious impact on operations, particularly in time-sensitive supply chain operations. The high percentage indicates the rising level and severity of ransomware attacks. To reduce the effects of such threats, organizations need to integrate regular data backups, endpoint protection and incident response plans.
- Insider Threats (15%): The insider threat makes up 15 percent of the total risk distribution, which involves risks of employees, contractors, or partners who have access to systems through the authorized means. Such threats can be either intentional like data theft, or unintentional like negligence or ignorance. Insider threats are the most dangerous threats, despite being less percentage-wise than other risks, because of the degree of access that insiders have. This emphasizes the need to minimize the internal vulnerabilities by means of access control, employee surveillance, and cybersecurity training.
- Data Breaches (18%): Data breach takes 18 percent of cybersecurity risks and includes unauthorized access to sensitive data like customer data, financial records, and intellectual property. Such breaches may happen in case of the poor security systems, ineffective encryption procedures, or effective cyberattacks. Data breaches are usually serious in the end, causing monetary losses, legal action and negative publicity. This percentage highlights the importance of using good data protection mechanisms such as encryption, secure storage and security audit.
- Third-party Risks (22%): The third-party risks contribute to 22% of the overall distribution as the vulnerability of outside vendors and partners is high. Third-party integrations are very important to supply chain systems and when they are not well handled, security gaps arise. Such risks are the result of poor security procedures, non-compliance or breached vendor systems. The percentage is very high, which highlights the significance of managing the vendor risk, such as conducting comprehensive security evaluations, ongoing monitoring, and specifying the requirements of vendor contracts in terms of cybersecurity standards.

4.3. Discussion

The results of the study clearly indicate that third-party risks and phishing attacks are the most significant cybersecurity threats affecting supply chain systems. The external dependence on third-party vendors, suppliers, and service providers can cause a critical situation because of the high prevalence of third-party risks as these actors usually have access to internal systems and access sensitive information. Such third parties might not be subjected to the same high level of security and this presents a weakness that can be exploited by cyber attackers. This risk is enhanced by the interdependence of supply chains where one weak point can affect the whole system. Furthermore, the lack of transparency in third-party security practices does not allow organizations to effectively monitor and

control possible threats. Conversely, phishing attacks are still very common because they are easy and effective in exploiting human weaknesses. Staff working in the procurement, as well as communication with external partners, is especially vulnerable to fake emails and fake links, which may result in stealing credentials and unauthorized access to the system. The prevalence of phishing attacks underscores the need to conduct user awareness and training and deploy sophisticated email filtering and authentication systems. Combined, these two risks show that technological and human factors contribute considerably to the cybersecurity of supply chains. The results indicate that organizations need to implement an integrated security strategy that will encompass a rigorous vendor risk management process, ongoing monitoring, and staff training. Moreover, the possibility to integrate modern technologies like artificial intelligence to detect threats may help to better detect and counteract them on the spot. In general, third-party risks and phishing attacks are crucial issues that should be addressed to improve the security and resilience of contemporary supply chain systems.

5. Conclusion

The research concludes that cybersecurity has become an essential part of the contemporary digitized procurement and supply chain systems, in which the growing dependency on digital technologies has greatly broadened the range of threats. With the integration of newer tools in the form of cloud computing, IoT tools, and automated procurement tools, organizations are also prone to a vast pool of cyber threats that can cause operations to be disrupted, sensitive data to be compromised, and damage organizational reputation. The results of this study underline the fact that cybersecurity is not just a supporting role but a strategic need, which should be incorporated into all levels of supply chain management. Among the most prominent findings of the research is the increased vulnerability of third-party integrations, and the very high rate of phishing and ransomware attacks. These threats are indicative of the need to consider both technology-related vulnerabilities and human aspects in cybersecurity policies.

In order to effectively reduce these risks, the research paper highly recommends a multi-layered security practice, also referred to as defense-in-depth. In this approach, there is the deployment of various security controls at various levels such as network, application, data and user access layers so that should one of the layers be compromised others are not compromised in order to safeguard the system. Important elements, including encryption, multi-factor authentication, constant monitoring, and implementing a Zero Trust model are critical to enhancing overall security. Moreover, organizations should put priority on vendor risk management by implementing a high level of security, regularly auditing vendors, and ensuring transparency with third-party partners. Training and awareness of the employees also plays a significant role in mitigating the social engineering attack, e.g. phishing.

Moreover, the research states the necessity to introduce the newest technologies, such as artificial intelligence and machine learning, to increase the threat detection and response capacities. Such technologies can offer real time insight and predictive analysis and help organizations to deal with potential threats proactively. To sum up, an all-encompassing, proactive, and dynamic cybersecurity model is needed to guarantee the resilience, reliability, and safety of digitized procurement systems in an ever-connected and risk-prone online setting.

References

[1] Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. International journal of production research, 57(3), 829-846..

[2] Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of information management, 39, 80-89.

[3] Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International journal of production research, 57(7), 2117-2135.

[4] Choi, T. M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. Production and operations management, 27(10), 1868-1883.

[5] Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342-353.

[6] Cybersecurity, C. I. (2014). Framework for improving critical infrastructure cybersecurity. Framework, 1(11), 1-55.

[7] Tang, O., & Musa, S. N. (2011). Identifying risk issues and research advancements in supply chain risk management. International journal of production economics, 133(1), 25-34.

[8] Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda. Supply Chain Management: An International Journal, 25(2), 223-240.

[9] Christopher, M., & Peck, H. (2004). Building the resilient supply chain.

[10] Chang, S. E., & Chen, Y. (2020). When blockchain meets supply chain: A systematic literature review on current development and potential applications. IEEE access, 8, 62478-62494.

[11] Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.
[12] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of computer and system sciences, 80(5), 973-993.
[13] Dhurandhar, A., Graves, B., Ravi, R., Maniachari, G., & Ettl, M. (2015, August). Big data system for analyzing risky procurement entities. In Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 1741-1750).
[14] Haimes, Y. Y. (2011). Risk modeling, assessment, and management. John Wiley & Sons.
[15] Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. Electronics, 9(11), 1864.
[16] Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. Future internet, 11(3), 63.
[17] Al-Farsi, S., Rathore, M. M., & Bakiras, S. (2021). Security of blockchain-based supply chain management systems: challenges and opportunities. Applied Sciences, 11(12), 5585.
[18] Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing, 13(1), 103-128.
[19] Aven, T. (2011). Quantitative risk assessment: the scientific platform. Cambridge university press.
[20] Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. Entropy, 25(12), 1595.
[21] Li, Y., & Xu, L. (2021). Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. International Journal of Production Research, 59(4), 1216-1238.